Kvadratne forme

↑ homogeni polinomi drugog stupnja s cjelobrojnim koef.

(binarne)

Primjer: $x^2+y^2 =: f(x,y)$

Q: $f(\mathbb{Z}\times\mathbb{Z}) = ?$

Gauss: $p = x^2+y^2$

↑ prost.

$5 = 1^2+2^2$

$7 = \times$

$11 = \times$

$13 = 2^2+3^2$

⋮

Teorem: $p = x^2+y^2 \iff p \equiv 1 \ (4)$

$\mathbb{Z}[i] = \{a+bi : a,b \in \mathbb{Z}\}$

↑ prsten cijel. Gauss.

$5 = (2+i)(2-i)$

$7 = 7$

$11 = 11$

$13 = (2+3i)(2-3i)$

$N : \mathbb{Z}[i] \to \mathbb{Z}$

$N(z) = |z|^2$

$N(\alpha_1 \cdot \alpha_2) = N(\alpha_1) N(\alpha_2)$

Q: Za koji proste $p \in \mathbb{Z}$

$\exists \alpha \in \mathbb{Z}[i]$ t.d.

$N(\alpha) = p$ ....

x^2+5y^2 ... ?

binarne kv. forme

$$f(x,y) = ax^2 + bxy + c^2 \,; \quad a,b,c \in \mathbb{Z} \iff f = [a,b,c]$$

ax^2+bx+c

$\downarrow$

$d = b^2 - 4ac$

$\uparrow$

diskriminanta

$$4 \cdot a\, f(x,y) = (2ax+by)^2 - d \cdot y^2$$

$\Rightarrow$ ako je $d<0$ pozitivna ili negativno definitna

ako je $d>0$ indefinitna

Def.: Kažemo da kvadratna forma reprezentira $n \in \mathbb{Z}$ ako postoji $x_0, y_0 \in \mathbb{Z}$ t.d. $f(x_0,y_0) = n$.

Ako pritom $(x_0,y_0)=1$, onda kažemo da je reprezentacija prava, inače je neprava.

Ideja: zamjena varijabli: $x = X + 2Y$; $Y = y - x$

$y = X + 3Y$; $X = 3x - 2y$

$x^2 + y^2$

$$(X+2Y)^2 + (X+3Y)^2 = 2X^2 + 10XY + 13Y^2$$

$\Rightarrow$ Kvadratne forme $[1,0,1]$ i $[2,10,13]$ reprezentiraju iste brojeve (imaju istu sliku) — reći ćemo da su ekvivalentne.

Def. Dvije kvad. forme f i g su ekviv. ako se jedna može transf. u drugu pomoću cjelobrojnih unimodularnih transf., tj. supstitucijom oblika

$$x = px' + qy' \qquad y = rx' + sy' \quad \text{gdje su}$$

$p, q, r, s \in \mathbb{Z}$ i $ps - qr = 1$. Pišemo $f \sim g$.

$ps - qr = 1$ ...

Propozicija. $\sim$ je relacija ekvivalencije

dokaz: dz.

$f = [a,b,c]$

$F = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$

$X = \begin{pmatrix} x \\ y \end{pmatrix}$

$f = X^T F X$

↑ matrični prikaz.

$U = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ .. $\det U = 1$; $U \in SL_2(\mathbb{Z})$

grupa 2×2, $\det = 1$

$f \sim g$

$F \quad G = U^T F U$

projekt: definiran djelom.

def: Kažemo da grupa G djeluje na skup X ako postoji fj. φ

$G \xrightarrow{\varphi} Perm(X)$ ← bijekcije $X \to X$

$g \longmapsto \varphi(g) = \underline{g}$; $x_1 \in X$, $\underline{g}\, x_1 \in X$

t.d. $\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2) \quad \forall g_1, g_2 \in G$

$\varphi(e) = I$.

grupe $SL_2(\mathbb{Z})$ na skupu matričnih prikaza kvadratnih formi.

Propozicija: Neka su $f \sim g$ i $n \in \mathbb{Z}$. Tada

1) f repr. $n \iff g$ repr. n
2) f pravo rep. $n \iff g$ pravo rep. n

} posljedica unimodularnosti (d.z.)

3) diskriminante od f i g su jednake.

$[a,b,c] = f \rightsquigarrow F = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \overset{U}{\rightsquigarrow} U^T F U = G \rightsquigarrow g$

$\operatorname{disc} f \rightsquigarrow \det F \cdot (-4)$

$\det(AB) = \det A \cdot \det B$

$\Rightarrow \det F = \det G$

(jer $\det U = 1$).

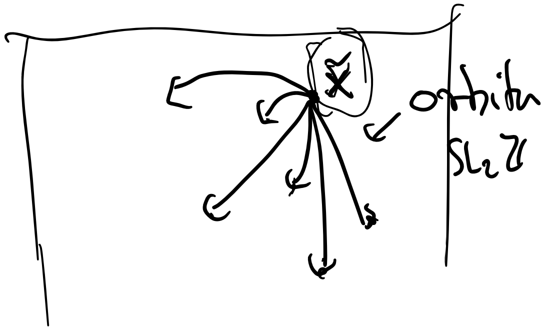
$x^2+y^2 \rightsquigarrow \operatorname{disc} = -4$

$\circlearrowleft SL_2(\mathbb{Z})$

Redukcija pozitivno def. kvadratnih formi.

$(d<0,\ a>0 \Rightarrow c>0)$

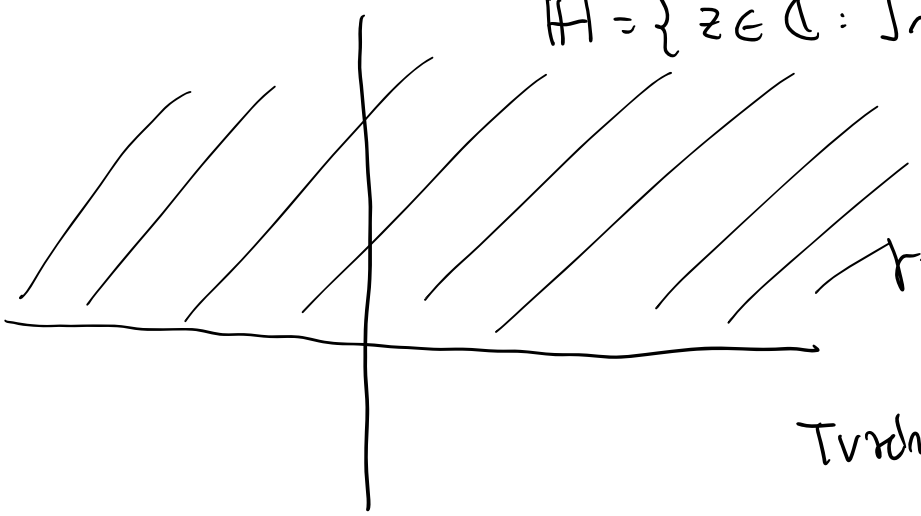
skup svih kv. formi disc $= -4$



Def: Reći ćemo da je pozit. def. kvadratna forma $f(x,y) = ax^2+bxy+c^2$ reducirana ako je

$-a < b \leq a < c$ ili $0 \leq b \leq a = c$

Teorem: Svaka pozitivno definitna kvadratna forma je ekvivalentna nekoj reducirnoj formi.



$\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}\, z > 0\}$ ↖ gornja poluravnina

$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \rightsquigarrow z \overset{\varphi_\gamma}{\longmapsto} \frac{az+b}{cz+d}$ ↙ Möbiusova transf.

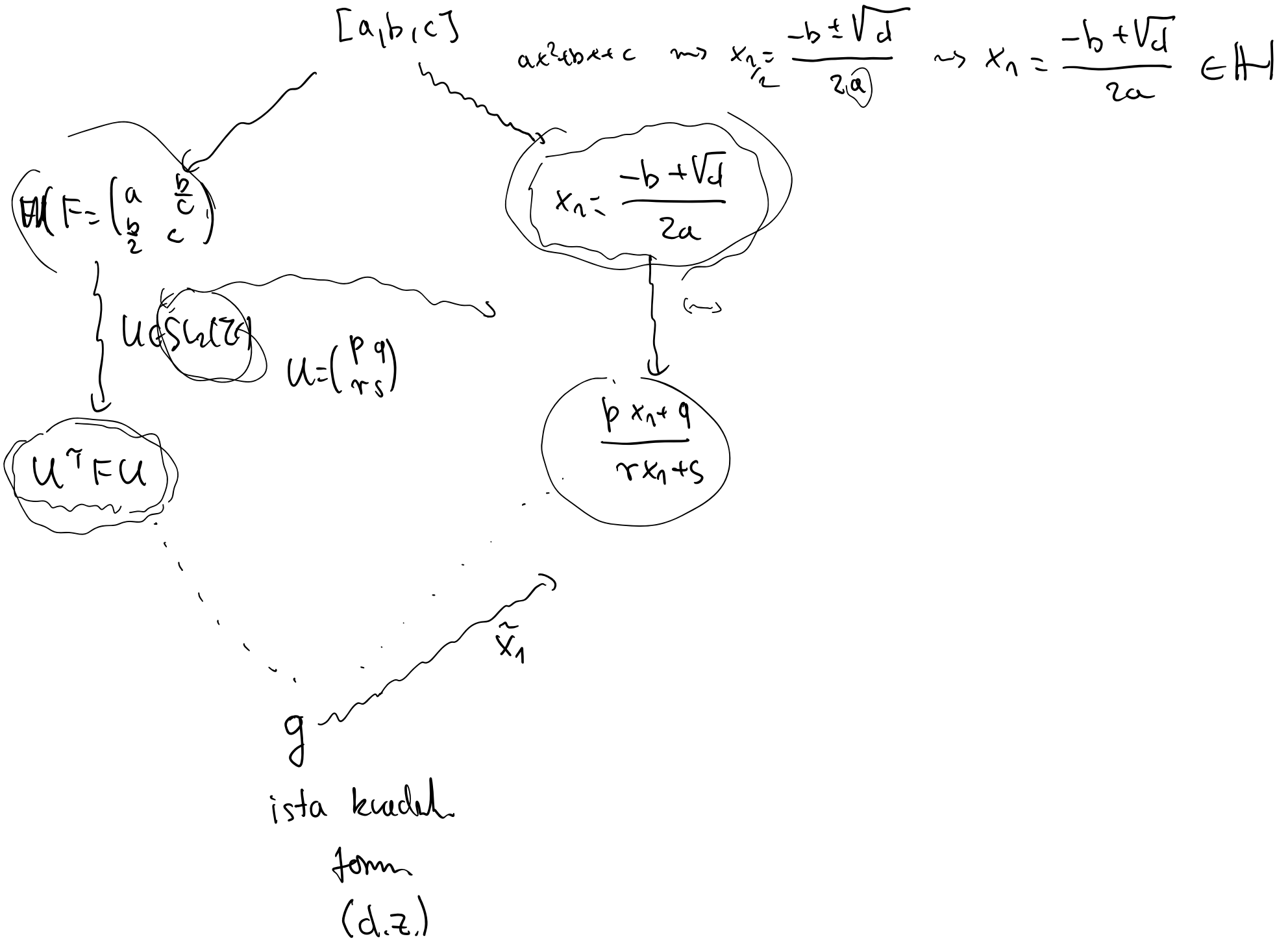
$\in \mathbb{H}$ ↙ komp.

Tvrdnja: • $\varphi_{\gamma_1} \circ \varphi_{\gamma_2} = \varphi_{\gamma_1 \cdot \gamma_2}$ $\forall \gamma_1, \gamma_2 \in SL_2(\mathbb{Z})$

↑ množenj matr.

• $\varphi_{I_d} = Id.$ (d.z.)

$\Rightarrow SL_2(\mathbb{Z})$ djeluje Möb. trans. na $\mathbb{H}$.


[a,b,c]
$ax^2+bx+c \rightsquigarrow x_{1/2} = \frac{-b \pm \sqrt{d}}{2a} \rightsquigarrow x_1 = \frac{-b+\sqrt{d}}{2a} \in \mathbb{H}$
$F = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$
$x_1 = \frac{-b+\sqrt{d}}{2a}$
$U \in SL_2(\mathbb{Z})$
$U = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$
$U^T F U$
$\frac{p x_1 + q}{r x_1 + s}$
$\tilde{x}_1$
g
ista kvadr. form
(d.z.)

Teorem 4.6. Neka su $d < 0$ i $n > 0$ cijeli brojevi. Tada je n pravo reprezentiran nekom binarnom kvadratnom formom s diskr. d ako i samo ako kongruencija $x^2 \equiv d \pmod{4n}$ ima rješenja.